



DEPARTMENT OF THE NAVY  
OFFICE OF THE CHIEF OF NAVAL OPERATIONS  
WASHINGTON, DC 20350-2000

IN REPLY REFER TO

5510

Ser N09N2/5U981060

OCT 3 2005

From: Chief of Naval Operations

Subj: ALTERNATIVE OR COMPENSATORY CONTROL MEASURES POLICY  
CHANGE NOTICE AND DATA CALL

Ref: (a) SECNAVINST 5510.36  
(b) OASD(C3I) memo of 18 Apr 03 (NOTAL)  
(c) NAVAUDSVC Report N2005-NAA000-0079.000 (NOTAL)

Encl: (1) Alternative or Compensatory Control Measures  
(ACCM) Policy Change Notice

1. Enclosure (1) provides advance notification of a policy change to reference (a) on the implementation of Alternative or Compensatory Control Measures (ACCM). Enclosure (1) will be incorporated in the next revision to reference (a). Reference (b) refers.

2. By reference (c), this office was requested to review current ACCM for compliance with current Department of Defense ACCM policy. If you are applying ACCM to classified information for which you are the original classification authority (OCA) OR if you have personnel with access to information to which ACCM have been applied by another OCA, please contact Ms. Bridget Ouellette at (202) 433-8847 or bouellet@ncis.navy.mil no later than 28 October 2005. Negative responses, in writing via email, are required.

3. Addressees are requested to forward this notice to all subordinate activities.

*B. A. Marshall*

B. A. MARSHALL  
Assistant for Information  
and Personnel Security

Subj: ALTERNATIVE OR COMPENSATORY CONTROL MEASURES POLICY CHANGE  
NOTICE AND DATA CALL

Distribution:

CNO (N09B11)  
COMLANTFLT  
COMPACFLT  
COMUSNAVEUR  
COMUSNAVCENT BAHRAIN  
COMFLTFORCOM  
COMNAVAIRSYSCOM  
COMNAVSEASYSYSCOM  
COMNAVFACENGCOM  
COMSPAWARSYSCOM  
COMNAVSECGRU  
COMSC  
COMNAVRESFOR  
BUPERS  
COMNAVDIST  
DIRSSP  
CNI  
ONI  
COMNAVLEGSVCCOM  
USNA  
NAVPGSCOL  
NAVWARCOL  
BUMED  
PRESINSURV  
NAVOBSY  
COMNAVSPECWARCOM  
NAVSTKAIRWARCEN  
COMOPTEVFOR  
NAVHISTCEN  
FLDSUPPACT  
NCTSI  
COMNAVSAFECEN  
COMNAVMETOCCOM  
COMNAVNETWARCOM  
NETC  
CNR  
AUDGEN  
NAVY JAG  
NAVCRIMINVSERV  
NAVY IPO  
CMC

## ALTERNATIVE OR COMPENSATORY CONTROL MEASURES (ACCM)

### 1. POLICY

a. When an Original Classification Authority (OCA) determines that other security measures detailed in SECNAVINST 5510.36 are insufficient for establishing "need-to-know" for classified information, and where Special Access Program (SAP) controls are not warranted, Alternative or Compensatory Control Measures (ACCM) may be employed. The purpose of ACCM is to strictly enforce the "need-to-know" principle. Additional security investigative or adjudicative requirements are not authorized for establishing access requirements for ACCM information.

b. The following ACCM controls are authorized:

(1) An unclassified nickname assigned in accordance with OPNAVINST 5511.37C **and** coordinated through CNO (N09N2).

(2) A list of persons authorized access.

(3) Placing classified ACCM information in sealed envelopes marked only with the classification level and nickname and stored in a manner to avoid commingling with other classified information.

(4) Special markings to identify information as being controlled by ACCM.

(5) A system that provides for recurrent oversight and inspection of ACCM by representatives of the cognizant OCA or CNO (N09N2).

c. ACCM Limitations:

(1) ACCM shall not use codewords as defined in OPNAVINST 5511.37C, nor shall they use the assigned nickname if it is not preceded by the acronym "ACCM."

(2) ACCM shall not be used for NATO or non-intelligence Foreign Government Information (FGI) without the prior written approval of the ODUSD (TSP&NDP). Any such request must be submitted via CNO (N09N2).

(3) ACCM shall not be used to protect classified information in acquisition programs as defined in DOD Directive 5000.1, nor shall ACCM be used during the acquisition process to protect technical or operational requirements of systems being acquired, weapon systems/end item characteristics, funding, capabilities or vulnerabilities.

(4) ACCM shall not be used to control classified information designated as Restricted Data (RD), Formerly Restricted Data (FRD), Communications Security (COMSEC) or Sensitive Compartmented Information (SCI).

(5) ACCM shall not be used for unclassified information.

(6) An ACCM specific Non-Disclosure Agreement shall not be used.

(7) The use of ACCM measures shall not preclude, nor unnecessarily impede, Congressional, Office of the Secretary of Defense, or other appropriate oversight of programs, command functions, or operations.

## **2. ESTABLISHMENT**

a. The CNO (N09N2) approves the use of ACCM, and ensures that the protection afforded classified information is sufficient to reasonably deter and detect loss or compromise. Each request for the establishment of ACCM shall consider the criticality, sensitivity, and value of the information; analysis of the threats both known and anticipated; vulnerability to exploitation; and countermeasures benefits versus cost when assessing the need to establish an ACCM.

b. Requests must be submitted, in writing, by the cognizant OCA. The request must include a justification

for application of ACCM and a security plan. The security plan shall describe how control measures will be implemented; identify the CNO (N09N2) approved nickname and describe how information will be marked with the nickname; provide a description of the information requiring additional control measures; and describe roles and responsibilities for implementation and oversight of the ACCM.

c. The CNO (N09N2) shall maintain a centralized record that, as a minimum, reflects the control(s) used and the rationale for their use, and shall report annually to the ODUSD (TSP&NDP) and ODUSD (CI&S). OCAs with approved ACCM shall provide program information as requested by CNO (N09N2) for inclusion in the report.

### **3. HANDLING AND SAFEGUARDING**

a. Markings. Nicknames for ACCMs (e.g., LIMIT FICTION) are assigned and approved via CNO (N09N2). The headers and footers of each applicable page of ACCM protected information shall identify the classification level and appropriate nickname (i.e., SECRET//LIMIT FICTION), in addition to the other markings required by SECNAVINST 5510.36, Chapter 6. These include warning notices, intelligence control markings and caveats, as appropriate. Similarly, each portion, part, paragraph and similar portion will, in addition to standard security classification markings, be marked with the ACCM nickname(s), e.g., (S/ACCM LIMIT FICTION). Only the full nickname may be used after the "ACCM" marking. No abbreviation of the nickname or any derivation of the nickname shall be used.

b. Safeguarding. Standard Form cover sheets may be used, but must be stamped or marked with the ACCM markings. The Director of Security, ODUSD (CI&S), via CNO (N09N2) may authorize the use of specially designed cover sheets.

c. Transmission. ACCM information shall be transmitted in the same manner as other classified information at the same classification level with the following exceptions:

(1) ACCM information wrapped for transmission shall have the inner envelope marked with the ACCM nickname and

must be addressed to the attention of an individual authorized access to the ACCM information.

(2) The ACCM nickname shall be used in the text of message traffic and on cover sheets accompanying secure FAX transmissions to assist in alerting the recipient that the transmission involves ACCM protected information. Senders shall ensure that an authorized recipient is awaiting the transmission when sending over secure FAX.

d. Automated Information Systems. Electronic files containing ACCM protected information shall be configured and designated to ensure that access is restricted to individuals with authorized access. SIPRNET or other secure transmission methods authorized for processing classified information at the same level may be used to transmit ACCM information. Each such transmission must be marked as described above, and transmitted only to those authorized access to the ACCM information.

e. Security Education. Personnel requiring access to ACCM protected information shall receive specialized training regarding the procedures for access, control, transmission, storage, marking, etc. Individuals may be required to sign an acknowledgement of training should the security plan so specify.

f. Contractors. Approved ACCM may be applied to cleared DoD contractors only when identified in the Contract Security Classification Specification, DD Form 254.

g. Security Plan. Activities and individuals having responsibility for protecting ACCM information (including contractors) shall be provided a copy of the ACCM security plan, as appropriate.

h. Security Classification Guide. The requirement for ACCM shall be included in security classification guides for the protected information.

**4. CANCELLATION.** ACCM shall be cancelled as soon as they are no longer necessary. Requests for cancellation must be submitted to CNO (N09N2), in writing. CNO (N09N2) will notify ODUSD (TSP&NDP) and ODUSD (CI&S).